



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,473	06/08/2001	John M. Davis	211139.90123	9874

29906 7590 05/12/2005
INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251

EXAMINER

ELMORE, JOHN E

ART UNIT PAPER NUMBER

2134

DATE MAILED: 05/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

1. In response to the previous office action, Applicant has amended claims 1, 5, 7, 8, 13-15 and 18. Claims 1-22 have been examined.

Claim Rejections - 35 USC § 112

2. In view of Applicant's amendment, the previous rejections under 25 U.S.C. 112 are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. **Claims 1, 3, 5-8, 10, 12, 13, 21 and 22 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad (USPN 6,157,955 – published December 5, 2000) in view of Nortel ("Using the Accelar 710 Server Switch," Nortel Networks, October 11, 1999, as cited in the IDS).

Regarding independent claim 1, Narad discloses an apparatus comprising
a proxy operable to receive a plurality of packets each including an
encrypted portion (apparatus receives a stream of packets to be processed, and since

Art Unit: 2134

processing can include decryption, packets can be received that have been encrypted from the sender; see column 6, line 46, through column 7, line 2),

the proxy operable to buffer the packets until a predetermined number of packets greater than one packet are received (ring array queues one or more received packets; Fig. 2, 3 and 7; col. 8, line 32, through col. 9, line 19; col. 18, line 12, through col. 19, line 12),

the proxy further operable to decrypt the encrypted portion of each received packet (column 9, lines 5-9) and forward the decrypted packets to a predetermined destination (TX ring forwards packet to original destination address; column 30, lines 42-43, and column 31, lines 15-25).

But Narad does not explain that the proxy is a proxy that handles Secured Sockets Layer (SSL) protocol transactions.

However, Nortel teaches an SSL proxy (accelerator) that processes SSL transactions for the purpose of reducing the workload on network servers (page xiii, paragraph 1; page 1-1, paragraph 1; page 2-1, paragraph 2; and page 2-5, paragraph 2).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad with the teaching of Nortel to provide a cryptographic coprocessor that can encrypt and decrypt packets in accordance with the SSL protocol. One would be motivated to do so in order reduce the workload of network servers that process SSL transactions.

Art Unit: 2134

Regarding dependent claim 3, Narad and Nortel further teach an apparatus wherein the encrypted portion of the packets are decrypted when received and the SSL proxy buffers the received packets out of order (encrypted packets placed in decryption queue when received while other packets may be forwarded out-of-order; column 30, lines 42-44 and section 7.2).

Regarding dependent claim 5, Narad and Nortel further teach an apparatus wherein the packets are sent by a client computer and received by a server computer (apparatus receives packet stream from client to server, processes it, and forwards to server; see column 6, lines 42-47; column 113, lines 41-55; and Figure 1), wherein the apparatus supports TCP/IP (col. 4, lines 64-67), and wherein the intended application for the apparatus includes web billing (col. 1, lines 32-41).

But the modified device of Narad and Nortel as applied to claim 1 does not explicitly explain a client computer running a web browser and a server computer running a web server.

However, Nortel teaches an apparatus that processes packets sent by a client computer and received by a web server computer for the purpose of increasing the performance of web sites (pages xiii and B-2). And it is well known in the art that a web server running on a server computer conducts transactions with a web browser running on a client computer. Therefore, it would be obvious to one of ordinary skill in the art at the time of the invention to modify the device of Narad and Nortel with the further teaching of Nortel such that the packets are sent by a client computer running a web

Art Unit: 2134

browser and received by a server computer running a web server. One would be motivated to do so in order to increase the performance of web sites.

Regarding dependent claim 6, Narad and Nortel are relied upon for teaching in regard to claims 1 and 5. Narad and Nortel further teach an apparatus wherein the SSL proxy is operable to receive unencrypted data from the server, encrypt the unencrypted data, and send the encrypted data to a client computer (apparatus receives a stream of packets to be processed, and since processing can include encryption, packets received can be unencrypted; also, the designations of client and server are interchangeable in that the proxy can receive packets from the sender and forward to the other regardless of which computer initiates the session between the two; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Regarding dependent claim 7, and Nortel further teach an apparatus wherein the SSL proxy performs encryption and decryption on packets using a single end-to-end TCP connection between a client computer and a server and the source and destination address of the packets are unaltered (apparatus processes packet stream between client and server on same TCP connection and performs encryption and decryption on packets; see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Regarding independent claim 8, Narad and Nortel are relied upon for teaching in regard to claims 1 and 5, particularly that the apparatus embodies the SSL protocol, that the client computer runs a web browser, that the server computer runs a web server, and that the received packets can contain encrypted payloads.

Art Unit: 2134

Narad and Nortel disclose a system for handling SSL traffic comprising:

a client computer running a web browser operable to initiate an SSL session and to send packets with encrypted payloads (apparatus receives packet stream of encrypted payloads from client to be decrypted; Narard, see column 6, lines 42-47; column 113, lines 41-55; and Figure 1).

a server computer running a web server operable to support communications with the client computer (server exists apart from apparatus and communicates with client; Narard, see column 6, lines 42-47; column 113, lines 41-55; column 7, lines 63-67; and Figure 1); and

a SSL proxy coupling the client computer and the server computer and operable to decrypt the encrypted payloads of each packet and forward the decrypted packets to the server computer (apparatus receives encrypted packet stream from client to server, decrypts it, and forwards to server; Narard, see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Dependent claim 10 is rejected on the same basis as claim 3 with reliance upon Narad and Nortel for teaching in regard to claim 8.

Regarding dependent claim 12, Narad and Nortel are relied upon for teaching in regard to claim 8. Narad and Nortel further teach an apparatus wherein the SSL proxy is operable encrypt packets sent from the server to the client computer (apparatus receives a stream of packets to be processed, and since processing can include decryption, packets received at proxy can be encrypted from the sender; also, the designations of client and server are interchangeable in that the proxy can receive

Art Unit: 2134

packets from the sender and forward to the other regardless of which computer initiates the session between the two; Narad, see column 6, line 42, through column 7, line 6; column 113, lines 41-55; and Figure 1).

Dependent claim 13 is rejected on the same basis as claim 7 with reliance upon Narad and Nortel for teaching in regard to claim 8.

Regarding independent claim 21, Narad teaches an apparatus for decrypting network data traffic comprising a proxy operable to:

(i) receive packets addressed to a server computer (see rationale for rejection of claim 5), the packets including an encrypted portion, a destination address, and a source address (apparatus supports TCP/IP which contains both a destination and a source address, and the payload can be encrypted; see column 6, line 42, through column 7, line 6; column 90, line 60, through column 91, line 15; column 104, lines 32-39; and Figure 1);

(ii) decrypt the encrypted portions of the received packets (column 6, line 42, through column 7, line 6); and

(iii) send the decrypted portions to a server computer without altering the destination or source address of the received packets (packets are intercepted at the OSI data link layer so the IP addresses remain unmodified when the packets are forwarded; see column 6, lines 46-48; column 7, line 63, through column 8, line 4; column 30, lines 42-44; column 31, lines 15-25; and column 104, lines 33-39).

Dependent claim 22 is rejected on the same basis as the rejection of claims 6 and 21.

Art Unit: 2134

2. **Claims 2 and 9 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel and further in view of Netscape ("Introduction to SSL," Netscape, October 9, 1998).

Regarding dependent claim 2, and Nortel further teach an apparatus that includes a database operable to track information about the packets (column 8, lines 16-19), including what cryptographic "operations to perform" on the packets (Crypto Command Descriptor; see column 16, lines 15-19, and column 27, lines 4-7) and the "encryption context" (column 36, lines 59-65), but Narad does not explicitly explain that this information includes a type of encryption scheme used to encrypt the encrypted portion of the packets.

However, Netscape teaches that the SSL protocol is capable of utilizing a number of alternative encryption types (page 2, last paragraph, and page 3, third paragraph).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of Netscape to include a database operable to track a type of encryption scheme used to encrypt the encrypted portion of the packets. The particular encryption scheme employed for each packet would be recorded, in the least, in the Crypto Command Descriptor, which describes to the cryptographic coprocessor the operations to perform on each packet. One would be motivated to do so in order to permit the cryptographic

Art Unit: 2134

coprocessor to handle a variety of encryption schemes in accordance with SSL protocol.

Dependent claim 9 is rejected on the same basis as claim 2 with reliance upon Narad and Nortel for teaching in regard to claim 8.

3. **Claims 4 and 11 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel and further in view of Bakhtiari et al, hereinafter Bakhtiari, ("A Message Authentication Code based on Latin Squares," Proceedings of Australasian Conference on Information Security and Privacy, 1997).

Regarding dependent claim 4, Narad and Nortel do not explicitly explain a proxy that tracks a message authentication code used to authenticate a message.

However, Bakhtiari teaches that a message authentication code is a common cryptographic tool composed of a checksum and a cryptographic key that is used to authenticate a message and verify that it has not been modified (page 1, first paragraph). Moreover, Narad and Nortel teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Narad and Nortel with the teaching of Bakhtiari to track a message authentication code used to authenticate a message. One would be motivated to do so in order to facilitate message authentication using a common method.

Art Unit: 2134

Dependent claim 11 is rejected on the same basis as claim 4 with reliance upon Narad and Nortel for teaching in regard to claim 8.

4. **Claims 14-18 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Narad and Nortel, further in view of Shostack ("An Overview of SSL," white paper, May 1995), and further in view of Po ("RFC 879 – TCP Maximum Segment Size and related topics," Network Working Group, 1983).

Regarding dependent claim 14, Narad and Nortel are relied upon in regard to the teaching in claim 8, but Narad and Nortel do not explain that the SL proxy buffers the packets until a predetermined number of packets arrive before decrypting the packets.

However, Shostack teaches that the SSL protocol is independent of TCP and that a transmitted message is fragmented into one or more encrypted records of up to 32,767 bytes each (page 1). And Po teaches that TCP segments (packets) vary in size depending on the Maximum Segment Size set by a receiving computer, with the long established practice in the art of setting the maximum segment size to 536 bytes (pages 1 and 2). One of ordinary skill in the art would recognize that multiple packets (TCP segments) would be required to transmit an encrypted SSL record where the record exceeds 536 bytes (not even considering the bytes required for the TCP header) and that such packets amount to a predetermined number which would need to be buffered before the message could be decrypted.

Therefore, the Examiner takes official notice that it would be obvious to a person of ordinary skill in the art at the time the invention was made that the device of Norad and Nortel buffers the packets until a predetermined number of packets arrive, then decrypts packets, and forwards the decrypted packets to the server. One would be motivated to do so in order to properly decrypt an SSL record that was fragmented into multiple packets after the record was encrypted.

Regarding independent claim 15, Narad and Nortel are relied upon for teaching in regard to claim 1, particularly that the method involves the processing of SSL packets. Narad and Nortel further teach a method comprising:

initializing an SSL session between a client computer and a SSL proxy (apparatus receives packet stream of encrypted payloads from client to be decrypted; see column 6, lines 42-47; column 113, lines 41-55; and Figure 1);

receiving a packet including an encrypted portion at the SSL proxy (since processing can include decryption, packets can be received that have been encrypted from the sender; see column 6, line 46, through column 7, line 2);

determining if the received packet is a SSL packet (PP determines the nature of the packet, and given the teaching of Nortel, can determine whether it is an SSL packet; see column 6, line 56, through column 7, line 6; column 8, lines 8-16; and column 59, lines 51-54);

placing the received packet in a hold queue (arriving packets are queued; see column 7, line 67, through column 8, line 8; and column 30, lines 42-48);

outputting the decrypted packets to a server computer (column 9, lines 5-9; column 30, lines 42-43, and column 31, lines 15-25).

But Narad and Nortel do not explicitly explain checking the hold queue to determine if all packets expected for a given record have arrived and decrypting the encrypted portion of each packet once all the packets expected for the given record have arrived.

However, Shostack teaches that the SSL protocol is independent of TCP and that a transmitted message is fragmented into one or more encrypted records of up to 32,767 bytes each (page 1). And Po teaches that TCP segments (packets) vary in size depending on the Maximum Segment Size set by a receiving computer, with the long established practice in the art of setting the maximum segment size to 536 bytes (pages 1 and 2). One of ordinary skill in the art would recognize that multiple packets (TCP segments) would be required to transmit an encrypted SSL record where the record exceeds 536 bytes (not even considering the bytes required for the TCP header) and that the hold queue would continue to receive such packets until all packets for that record were received, as SSL decryption operates on the entire record.

Therefore, the Examiner takes official notice that it would be obvious to a person of ordinary skill in the art at the time the invention was made that the device of Norad and Nortel checks the hold queue to determine if all packets expected for a given record have arrived and decrypts the encrypted portion of each packet once all the packets expected for the given record have arrived. One would be motivated to do so in order to

Art Unit: 2134

properly decrypt an SSL record that was fragmented into multiple packets after the record was encrypted.

Dependent claim 16 is rejected on the same basis as claim 4 with reliance upon Narad and Nortel for teaching in regard to claim 15.

Regarding dependent claim 17, Narad and Nortel further teach that non-SSL packets are sent directly to the server (packets, especially those not requiring cryptographic processing, can be forwarded directly to the destination address; see column 30, lines 42-48, and column 31, lines 14-24).

Regarding dependent claim 18, Narad and Nortel further teach that the step of placing the packets in a hold queue comprises:

placing packets received out of order in a queue (out of order received packets can be queued for processing by the Policy Engine; see column 7, line 63, through column 8, line 4; column 31, lines 1-4; column 109, lines 3-6; and column 111, lines 25-35); and

decrypting packets received in order and forwarding the decrypted packets to a server computer (decryption is performed in order as PE can examine packets by sequence number before making them available to cryptographic coprocessor; see column 8, lines 9-13; column 60, line 50-53; column 61, lines 58-62; column 107, 58-60; column 108, line 24-58; and column 110, lines 58-67);

checking the hold queue to determine if the packet in the queue is next in sequence (column 108, line 63, through column 109, line 6);

releasing the packet from the hold queue if the packet in the queue is the next in sequence (column 108, line 63, through column 109, line 6; and column 110, lines 58-67); and

getting a new packet if the packet in the hold queue is not the next in sequence (PE can pass packet directly to cryptographic coprocessor by checking sequence number of arriving packets with the next expected sequence number in the queue; see column 31, lines 1-4 and 29-32; column 108, line 24, through column 109, line 6; and column 110, lines 58-67).

Dependent claim 19 is rejected on the same basis as claim 7 with reliance upon Narad and Nortel for teaching in regard to claim 15.

Dependent claim 20 is rejected on the same basis as claim 6 with reliance upon Narad and Nortel for teaching in regard to claim 15.

Response to Arguments

3. Applicant's arguments filed 15 February 2005 have been fully considered but they are not persuasive.

Regarding Applicant's argument that the combination of Narad and Nortel is improper due to lack of motivation, Narad teaches a general purpose packet processing device for the purpose of reducing the workload on network servers, which is also adaptable and "highly programmable" to accelerate various applications as needed (col. 3, lines 46-48; col. 6, lines 42-60). Nortel teaches a packet processing device used to accelerate SSL transactions for the purpose of reducing the workload on network (Web)

Art Unit: 2134

servers (Nortel, page xiii). The motivation for combining Narad with Nortel stems from the fact that both devices are packet processors aimed at reducing the workload of network servers and that Nortel teaches the particular application of accelerating SSL transactions for which the adaptability and programmability of the device of Narad is designed to encompass.

Applicant's argument that Narad "is drawn to a device that operates at the local area network level" while Nortel "discloses a hardware switch" (Remarks, page 8) is inconsequential to the function of each device as a packet processor. The Applicant makes no claim that the device must be a switch operating at the OSI data link layer. Neither does the SSL protocol require it.

Further, Applicant's argument that Narad teaches away from the Narad/Nortel combination hinges on the false assumption that the Narad/Nortel combination results in a modified device that is operable exclusively for one specific application. But in fact the modified device is still a general purpose packet processor capable of being adapted and programmed to suit other applications besides the acceleration of SSL transactions. Narad criticized the use of "typical" switches at the time of his invention because they were inadaptable besides lacking in sufficient processing power and facilities (Narad, col. 3, lines 25-35). This criticism does not teach away from the combination, even though the modified device of Narad and Nortel may be employed for the specific application of accelerating SSL transactions. To the contrary, it can be argued that the modified general purpose packet processing device provides an advantage in certain network environments because it not only accelerates SSL

Art Unit: 2134

transactions but also can also be adapted for other applications at less expense than replacing a fixed-use device.

Regarding Applicant's argument that "the buffer of Narad holds but one packet" (Remarks, page 9), Narad teaches a plurality of incoming packets buffered in a ring buffer (Fig. 2; col. 8, line 41, through col. 9, line 19). Narad's teaching that the receive data buffer "is a 2KB structure which contains an Ethernet packet and information about that packet," as quoted by Applicant (Remarks, page 9), should not be read to mean that only one packet is buffered at a time by the device. Rather, the device maintains one or more packet buffers (620) (which Narad also refers to as ring buffers) simultaneously in memory (260) structured as a ring array, allocating a new packet buffer to memory as each packet is received at RX MAC (216) (Narad, Fig. 3 and 7; col. 18, line 62, through col. 19, line 9). An MFILL buffer pointer is incremented for each packet received to mark the memory location of the latest packet, which also signals the Classification Engine (238) that a new packet is waiting to be processed. Narad particularly points out that "the ring array contains the buffer pointers to one or more full, unclassified buffers" representing one or more packets received by the RX MAC and awaiting processing by the Classification Engine (col. 19, lines 9-12). Moreover, the Classification Engine may delay processing on any packet in the receive buffer, which would leave one or more packets in memory (260) until they are later processed (col. 9, lines 16-19).

Regarding Applicant's argument that the Narad/Nortel combination fails to disclose, teach, or suggest that the proxy "performs encryption and decryption on

Art Unit: 2134

packets using a single end-to-end TCP connection between a client computer and a server and the source and destination address of the packets are unaltered," it is an inherent feature of the modified device that its processing of SSL packets, including encrypting and decrypting, does not alter the source and destination address of the packets. Applicant refers to Narad's teaching that "the RX MAC 220 or 228 places that packet at an offset" as support for the argument that as a consequence of offsetting the packet in the buffer (260), the "packet offsets the header, which is an alteration to the source and destination address" (Remarks, p. 10). However, offsetting the packet in the buffer does not alter the source and destination addresses for two reasons.

First, offsetting the packet in the buffer does not alter the contents of the Ethernet header of the packet, which would include the MAC source and destination addresses; rather, it merely adds padding in order for the packet to be word aligned for ease of processing within the device (col. 20, lines 26-37; col. 24, lines 10-17). Narad recognizes that the Ethernet header begins at the offset and subsequent transmission of the packet by TX MAC (222 or 223) and preserves the packet header and payload without alteration (col. 24, lines 10-66). Whether the packet is considered to be encapsulated during processing by the Narad device is irrelevant because the padding is removed at transmission and the format of the packet header is thus restored to what it was when initially received by the device.

Second, offsetting the packet in the buffer does not alter the contents of the packet payload, so IP source and destination addresses encapsulated therein are likewise unaltered. It is well known in the art that for TCP/IP transactions over a

Art Unit: 2134

Ethernet local area network, an Ethernet frame in its data field encapsulates an IP frame, the header of which contains IP source and destination addresses. Therefore, the Narad/Nortel combination processes SSL transactions without altering the IP source and destination addresses.

Further, Applicant's argument that Narad teaches the capability of altering the source and destination addresses is inconsequential because the modified device of Narad and Nortel does not necessitate any alteration of the source and destination addresses. As a general purpose device, Narad teaches the use of an Application Services Library (ASL) to program the device in adapting it to whatever packet processing an application requires, including a C/C++ library that provides network address translation services (col. 79, lines 23-38; col. 104, lines 33-39). But the Narad/Nortel combination simply operates to accelerate SSL transactions and in that embodiment requires no network translation services. Reprogramming the modified device to perform such address alteration would characterize a different application.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not

Art Unit: 2134


mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE



GREGORY
SUPERVISORY
TECHNOLOGY

